

# **IMPLEMENTASI RSA ALGORITHM DAN CYRPTOGRAPHY QUANTUM PADA SISTEM LOGIN**

## **TUGAS AKHIR**

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1

Teknik Informatika Universitas Muhammadiyah Malang



Oleh :

**Ridwan Annas pryagung**

**201510370311077**

**PROGRAM STUDI TEKNIK INFORMATIKA**

**FAKULTAS TEKNIK**

**UNIVERSITAS MUHAMMADIYAH MALANG**

**2019**

LEMBAR PERSETUJUAN

**IMPLEMENTASI RSA ALGORITHM DAN CYRPTOGRAPHY  
QUANTUM PADA SISTEM LOGIN**

Diajukan Untuk Memenuhi  
Persyaratan Guna Meraih Gelar Sarjana Strata 1  
Teknik Informatika Universitas Muhammadiyah Malang

**Ridwan Annas Pryagung**  
201510370311077

Menyetujui,

Dosen I



Aminudin, S.Kom, M.Cs  
NIDN. 0701068603

Dosen II



Sofvan Arifianto, S.Si, M.Kom  
NIDN. 0721058309

## LEMBAR PENGESAHAN

### IMPLEMENTASI RSA ALGORITHM DAN CYRPTOGRAPHY QUANTUM PADA SISTEM LOGIN

Diajukan Untuk Memenuhi  
Persyaratan Guna Meraih Gelar Sarjana Strata I  
Teknik Informatika Universitas Muhammadiyah Malang

**Ridwan Annas Pryagung**

201510370311077

Menyetujui,

Penguji I



Didih Rizki S.kom, M.kom

NIDN. 0702109201

Penguji II



Wildan Suharso S.kom, M.kom

NIDN. 0730038405

Mengetahui

Ketua Program Studi Teknik Informatika



Gita Indah Marthasari, ST., M.Kom.

NIDN. 720038101

## LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Ridwan Annas pryagung  
Tempat, Tanggal Lahir : Kediri, 07 april 1996  
NIM : 201510370311077  
Fakultas/ Jurusan : Teknik/ Informatika

Dengan ini saya menyatakan bahwa Tugas Akhir dengan judul "IMPLEMENTASI RSA ALGORITHM DAN CYRPTOGRAPHY QUANTUM PADA SISTEM LOGIN" beserta isinya adalah karya penulis sendiri dan bukan merupakan karya tulisan orang lain, baik sebagian atau seluruhnya, kecuali bentuk kutipan yang telah disebutkan sumbernya.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya. Apabila kemudian ditemukan adanya pelanggaran terhadap etika keilmuan dala karya saya ini, atau ada klaim dari pihak lain terhadap keaslian karya saya ini maka saya siap menanggung segala bentuk resiko atau sanksi yang berlaku.

Mengetahui,  
Dosen Pembimbing



Aminudin, S.Kom, M.Cs

NIDN. 0701068603

Malang, 30 September 2019



Ridwan Annas Prvagung

NIM. 201510370311077

## KATA PENGANTAR

Puji syukur kehadiran Allah Subhanahu Wa Ta'ala atas limpahan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan tugas akhir yang berjudul Implementasi RSA Algorithm dan Cryptography Quantum pada Sistem Login. Tulisan ini disajikan pokok-pokok bahasan mengenai algoritma RSA standar, improvisasi RSA, dan Quantum kriptografi mulai cara kerja, performa waktu, celah keamanan hingga pengembangannya. Selain itu juga dijelaskan mengenai pengaplikasian, pengujian waktu serta pengujian keamanan algoritma RSA standar, improvisasi RSA, dan Quantum Kriptografi. Peneliti menyadari sepenuhnya bahwa dalam penulisan tugas akhir ini masih banyak kekurangan dan keterbatasan. Oleh karena itu, peneliti sangat mengharapkan saran yang membangun agar tulisan ini bermanfaat untuk perkembangan ilmu pengetahuan kedepan.

Malang, 30 September 2019

Penulis

Ridwan Annas Pryagung

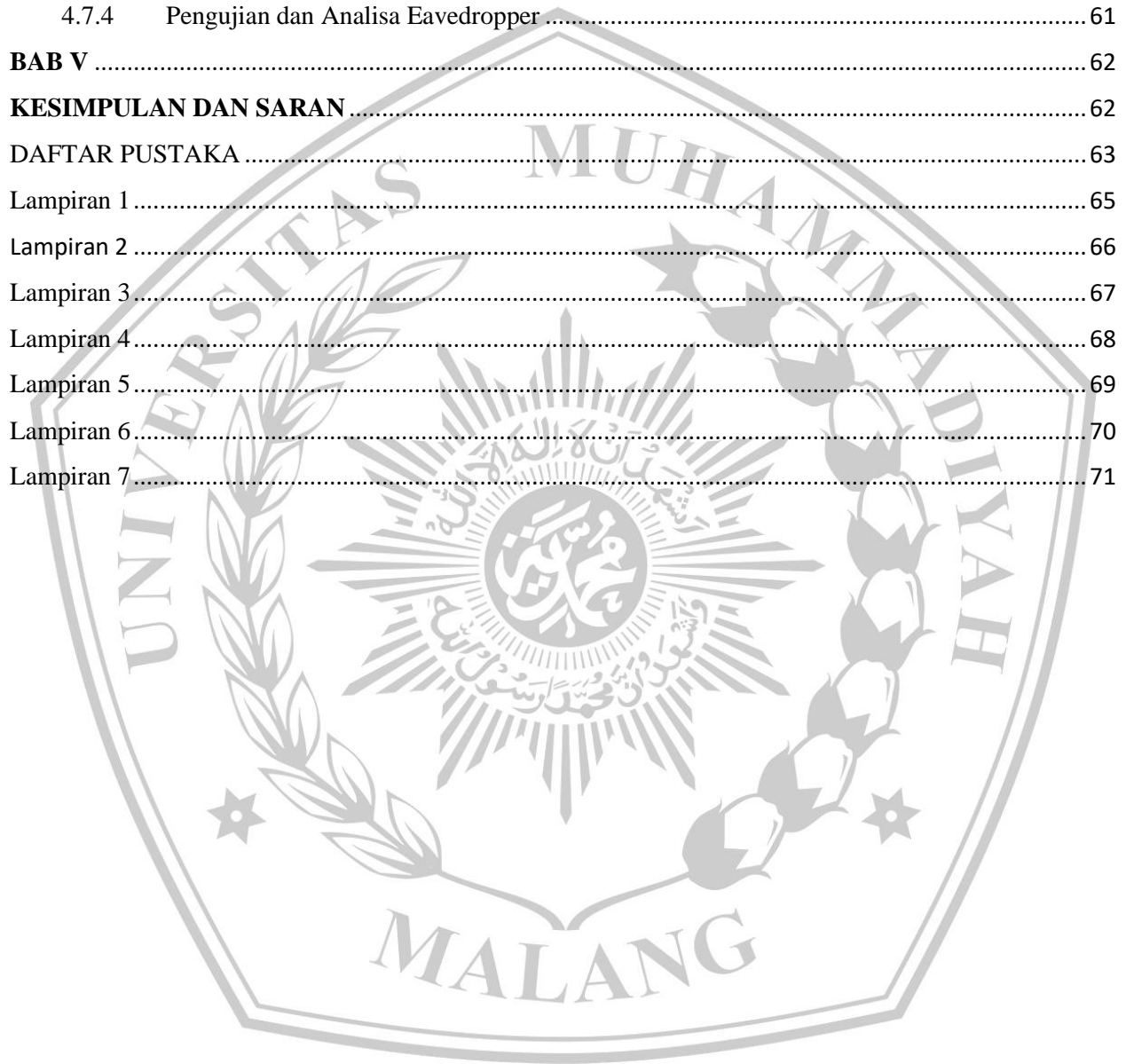
# DAFTAR ISI

LEMBAR PERSETUJUAN .....	i
LEMBAR PENGESAHAN .....	ii
LEMBAR PERNYATAAN.....	ii
ABSTRAK.....	iv
ABSTRACT.....	v
<b>LEMBAR PERSEMBAHAN</b> .....	vi
<b>KATA PENGANTAR</b> .....	vii
DAFTAR ISI.....	viii
Daftar Gambar .....	xi
Daftar Tabel .....	xii
Daftar Lampiran.....	xiii
BAB I.....	1
PENDAUULUAN .....	1
1.1    Latar Belakang .....	1
1.2    Rumusan Masalah.....	3
1.2    Tujuan Penelitian .....	3
1.3    Batasan Masalah .....	4
1.3    Penyusunan Laporan.....	4
1.4    Sistematika Penelitian.....	4
BAB II.....	7
TINJAUAN PUSTAKA .....	7
2.1    Bilangan Prima.....	7
2.1    Algoritma RSA .....	7
2.2    Kriptotografi Quantum.....	9
2.3    Penggabungan Algoritma RSA menggunakan Kriptografi Quantum.....	11
2.4    Fermat Factorization .....	13
2.6    Eavedropper .....	13
2.7    Jurnal terkait.....	14
2.7.1    Pengujian terhadap aplikasi algoritma RSA .....	14
2.7.2    Pengujian waktu algoritma RSA.....	14

2.7.3	Pengujian keamanan algoritma RSA menggunakan fermat factorization .....	16
2.7.4	Pengujian keamanan sistem login .....	16
BAB III .....		17
METODE PENELITIAN .....		17
3.1	Analisa masalah .....	17
3.2	Rancangan Algoritma RSA Standar .....	17
3.2.1	Pembangkitan kunci algoritma RSA standart .....	17
3.2.2	Enkripsi algoritma RSA Standart .....	19
3.2.3	Dekripsi algoritma RSA Standart .....	20
3.2.4	Rancangan kriptografi Quantum .....	22
3.3	Rancangan Improvisasi Algoritma RSA dengan Quantum kriptografi .....	23
3.3.1	Rancangan pembangkitan Improvisasi algoritma RSA dan kriptografi Quantum .....	23
3.3.2	Rancangan enkripsi Improvisasi algoritma RSA dan kriptografi Quantum .....	26
3.3.3	Rancangan dekripsi Improvisasi algoritma RSA dan kriptografi Quantum .....	28
3.3.4	Rancangan sistem registrasi menggunakan Algoritma RSA dan Kriptografi Quantum .....	29
3.3.5	Rancangan login menggunakan Algoritma RSA dan kriptografi Quantum .....	30
3.4	Rancangan Fermat Factorization .....	32
3.5	Eaveddropper .....	33
3.6	Skenario pengujian .....	34
3.6.1	Skenario pengujian terhadap aplikasi .....	34
3.6.2	Skenario pengujian peforma .....	35
BAB IV .....		46
IMPLEMENTASI DAN PENGUJIAN .....		46
4.1	Impelentasi .....	46
4.2	Implementasi perangkat keras .....	46
4.3	Implementasi Perangkat lunak .....	46
4.4	Implementasi Algoritma RSA .....	46
4.4.1	Implementasi Pembangkitan Kunci RSA .....	46
4.4.2	Implementasi Enkripsi Algoritma Standart .....	48
4.4.3	Implementasi Dekripsi Algoritma Standart .....	49
4.5	Implementasi pengabungan RSA dengan kriptografi quantum .....	50
4.5.1	Implementasi Pembangkitan Kunci RSA dan Kriptografi Quantum .....	50
4.5.2	Implementasi Enkripsi RSA dan Kriptografi Quantum .....	51



4.5.3	Implementasi Dekripsi RSA dan Kriptografi Quantum.....	52
4.5	Implementasi Fermat Factoriation .....	53
4.6	Pengujian.....	55
4.7.1	Pengujian Terhadap Aplikasi .....	55
4.7.2	Pengujian dan Analisa Fermat Factorization .....	59
4.7.4	Pengujian dan Analisa Eavedropper .....	61
<b>BAB V</b>	.....	62
<b>KESIMPULAN DAN SARAN</b>	.....	62
<b>DAFTAR PUSTAKA</b>	.....	63
Lampiran 1	.....	65
Lampiran 2	.....	66
Lampiran 3	.....	67
Lampiran 4	.....	68
Lampiran 5	.....	69
Lampiran 6	.....	70
Lampiran 7	.....	71





## Daftar Gambar

Gambar 2.1 skema algoritma RSA .....	8
gambar 3.1 pseudocode pembangkitan kunci algoritma RSA standar .....	19
gambar 3.2 alur pembangkitan kunci algoritma RSA .....	20
Gambar 3.3 pseudocode enkripsi algoritma RSA standar .....	22
gambar 3.4 alur enkripsi algoritma RSA standart .....	22
Gambar 3.5 pseudocode dekripsi algoritma RSA standar .....	24
gambar 3.6 alur Dekripsi algoritma RSa standart .....	24
gambar 3.7 alur quantum kriptografi .....	25
gambar 3.9 pseudocode pembangkitan kunci RSA dengan Quantum kriptografie .....	28
gambar 3.10 flowchart pembangkitan kunci RSA dengan quantum kriptografi .....	29
gambar 3.11 pseudocode enkripsi improvisasi RSA dengan Quantum kriptografi .....	32
gambar 3.12 flowchart enkripsi improvisasi RSA dengan quantum kriptograafi .....	33
gambar 3.13 pseudocode Dekripsi Imrovisasi algoritma RSA dan kriptografi Quantum .....	35
gambar 3.14 flowchart dekripsi Improvisasi RSA dengan quantum kriptografi .....	36
gambar 3.15 flowchart rgristrasi login sistem .....	37
Gambar 3.16 flowchart rancangan login dengan RSA dan Quantum kriptografi .....	38
gambar 3.17 flowchart alur fermat factorization .....	40
Gambar 3.18 simulasi penyerangan eavesdropper .....	41
Gambar 4.1 pseudocode enkripsi algoritma RSA standart .....	56
gambar 4.2 pseudocode enkripsi algoritma RSA standart .....	57
gambar 4.3 pseudocode dekripsi algoritma tandart .....	58
gambar 4.4 pseudocode implementasi pembangkitan kunci RSA dengan quantum.....	60
gambar 4.5 source kode impelemntasi RSA engan quantum .....	62
gambar 4.6 source kode implementasi dekripsi RSA dengan quantum .....	63
gambar 4.7 source kode fermat factorization .....	65

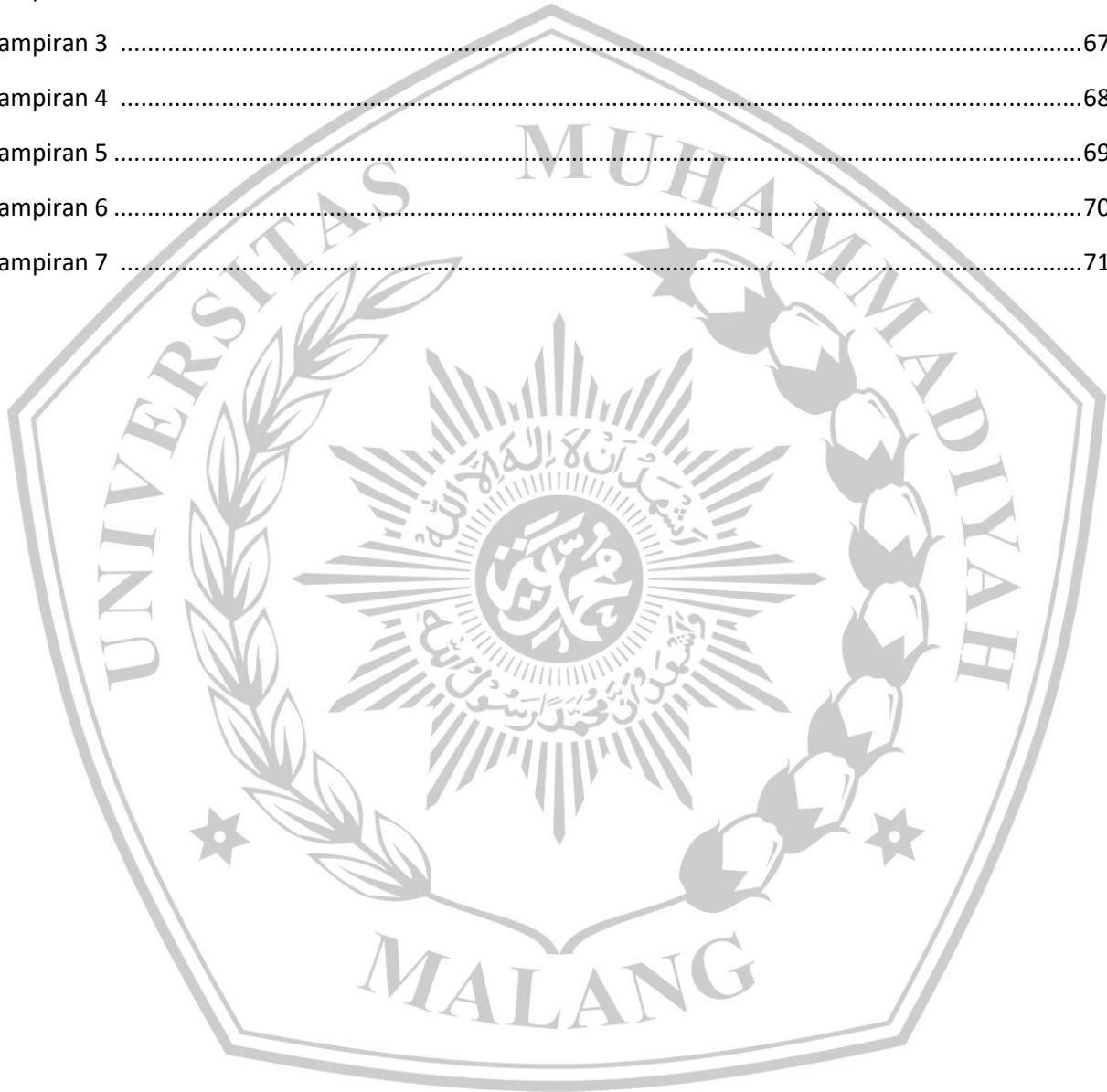
## Daftar Tabel

Tabel 3.1 skenario pengujian algoritma terhadap aplikasi .....	42
Tabel 3.2 skenario perbandingan waktu .....	45
Tabel 3.3 skenario perbandingan waktu enkripsi .....	46
Tabel 3.4 skenario perbandingan waktu dekripsi .....	47
Tabel 3.5 skenario pengujian fermat factorization .....	50
Tabel 3.6 skenario hasil pengujian fermat factorization .....	51
Tabel 3.7 skenario pengujian Eavedropper .....	53
Tabel 3.8 skenario hasil pengujian .....	53
Tabel 4.1 hasil pengujian terhadap aplikasi .....	66
Tabel 4.2 hasil pengujian pembangkitan kunci .....	68
Tabel 4.3 hasil pengujian waktu enkripsi .....	69
Tabel 4.4 hasil pengujian waktu dekripsi .....	70
Tabel 4.5 hasil pengujian fermat factorization .....	71
Tabel 4.6 hasil pengujian eavesdropper .....	72



## Daftar Lampiran

Lampiran 1 .....	65
Lampiran 2 .....	66
Lampiran 3 .....	67
Lampiran 4 .....	68
Lampiran 5 .....	69
Lampiran 6 .....	70
Lampiran 7 .....	71



## DAFTAR PUSTAKA

- [1] Paryati, "Keamanan SIM," vol. 2008, no. semnasIF, pp. 379–386, 2008.
- [2] A. D. Laksono and S. Kom, "Keamanan Sistem Komputer," pp. 1–11, 2017.
- [3] D. Ganguly and S. Lahiri, *Cryptography and Network Security*. 2012.
- [4] M. Bhavsingh, M. S. Lakshmi, S. P. Kumar, and N. Parashuram, "Improved Trial Division Algorithm by Lagrange " s Interpolation Function," no. May, pp. 1227–1231, 2017.
- [5] P. Pajic, "Quantum Cryptography," pp. 1–6, 2013.
- [6] B. S. Muchlis, M. A. Budiman, and D. Rachmawati, "Teknik Pemecahan Kunci Algoritma Rivest Shamir Adleman (RSA) dengan Metode Kraitichik," *SinkrOn*, vol. 2, no. 2, pp. 49–64, 2017.
- [7] K. Anggit, "The implementation of Asymmetric Algorithms Dual Modulus RSA in Applications Chat." pp. 1–9, 2018.
- [8] J. Informatika, F. Teknik, and U. M. Malang, "Analisa Hybrid Kriptosistem RSA dan EL-GAMAL pada Instant Messaging berbasis socket TCP," no. 09560491, 2018.
- [9] L. Ming-xin and K. Feng, "IJ " I Ja I," no. Iccasm, pp. 35–37, 2010.
- [10] K. Somsuk, "Higher Security for Login System Using RSA and One-time Pad Schemes," vol. 10, no. 1, pp. 99–103, 2018.
- [11] M. Ihwani, "Model Keamanan Informasi Berbasis Digital Signature Dengan Algoritma Rsa," *CESSJournal Comput. Eng. Syst. Sci.*, vol. 1, no. 1, pp. 15–20, 2016.
- [12] E. R. Sardju, R. Magdalena, and R. D. Atmaja, "Implementasi Algoritma Rsa Untuk Enkripsi Dan Dekripsi Sms (short Message Service) Pada Ponsel Berbasis Android," *eProceedings Eng.*, vol. 2, no. 2, pp. 2435–2442, 2015.
- [13] D. Wulansari, "Implementation of RSA Algorithm with Chinese Remainder Theorem for Modulus N 1024 Bit and 4096 Bit," no. 10, pp. 186–194.
- [14] N. Somani and D. Mangal, "An Improved RSA Cryptographic System," *Int. J. Comput. Appl.*, vol. 105, no. 16, pp. 975–8887, 2014.
- [15] S. Kromodimoeljo, *Teori&aplikasi kriptografi*. SPK IT Consulting.
- [16] H. R. Sandityas, "Analisa Hybrid Kriptosistem RSA dan EL-GAMAL pada Instant Messaging berbasis socket TCP," Malang, 2018.
- [17] M. V Pawar and J. Anuradha, "Network Security and Types of Attacks in Network," *Procedia - Procedia Comput. Sci.*, vol. 48, no. Iccc, pp. 503–506, 2015.
- [18] N. Fahriani, P. A. R. Devi, and D. Aditama, "Alternatif Penanganan Jenis Serangan Pencurian Data Pada Jaringan Komputer," no. November, pp. 24–25, 2017.
- [19] J. Ilmiah, I. Komputa, A. A. Zabar, F. Novianto, J. Dipatiukur, and C. Fax, "KEAMANAN HTTP DAN HTTPS BERBASIS WEB MENGGUNAKAN SISTEM OPERASI KALI LINUX Program Studi Teknik Komputer – FTIK Universitas

Komputer Indonesia Jurnal Ilmiah Komputer dan Informatika ( KOMPUTA ),” vol. 4, no. 2, 2015.

- [20] D. Email, A. Ginting, R. R. Isnanto, and I. P. Windasari, “Implementasi Algoritma Kriptografi RSA untuk,” vol. 3, no. 2, pp. 253–258, 2015.
- [21] and R. U. Rachmawati and A Budiman, “The cryptanalysis of the Rabin public key algorithm using the Fermat factorization method The cryptanalysis of the Rabin public key algorithm using the Fermat factorization method,” 2019.
- [22] A. Khairan, M. Imrona, and I. Ummah, “ANALISIS DAN IMPLEMENTASI KRIPTOGRAFI RSA PADA APLIKASI CHATTING CLIENT-SERVER BASED,” pp. 1–7.
- [23] D. M. Khairina, “ANALISIS KEAMANAN SISTEM LOGIN,” vol. 6, no. 2, pp. 64–67, 2011.





**UNIVERSITAS MUHAMMADIYAH MALANG**  
**FAKULTAS TEKNIK**  
**PROGRAM STUDI TEKNIK INFORMATIKA**  
 Jl. Raya Tlogomas 246 Malang 65144 Telp. 0341 - 464318 Ext. 247, Fax. 0341 - 460782

**FORM CEK PLAGIARISME LAPORAN TUGAS AKHIR**

Nama Mahasiswa : Ridwan Annas Pryagung  
 NIM : 201510370311077  
 Judul TA : IMPLEMENTASI RSA ALGORITHM DAN CYRPTOGRAPHY QUANTUM  
 PADA SISTEM LOGIN

Hasil Cek Plagiarisme dengan Turnitin

No.	Komponen Pengecekan	Nilai Maksimal Plagiarisme (%)	Hasil Cek Plagiarisme (%) *
1.	Bab 1 – Pendahuluan	10 %	2%
2.	Bab 2 – Kajian Pustaka	25 %	16%
3.	Bab 3 – Analisis dan Perancangan	25 %	11%
4.	Bab 4 – Implementasi dan Pengujian	15 %	14%
5.	Bab 5 – Kesimpulan dan Saran	5 %	5%
6.	Makalah Tugas Akhir	20%	7%

Mengetahui,

Dosen Pembimbing



(Sofyan Arifianto, S.Si, M.Kom)

\*) Hasil cek plagiarism bisa diisikan oleh salah satu pembimbing